

1.4 Neustar's Security Program

Why Neustar

- Security-Related Information
- Neustar security program uses the "defense-in-depth" approach, leveraging multiple layers of security to ensure system and information resiliency
- Neustar adheres to industry best practices for securing information and systems
- Continued training and education for security experts to remain ahead of emerging cyber threats, and ongoing Information Security training and awareness campaigns for all Neustar employees
- Security operations are all based in the United States

New for the Next Term

- Improved "threat intelligence" and response capability for NeuCIRT/SOC in 2013
- ISO27001 information security certification for NPAC
- Continued investment in the Information Security program to ensure Neustar stays ahead of emerging threats (people, processes, and technologies)

Neustar's approach to information security is a comprehensive, defense-in-depth program designed to mitigate all types of information security risks, while constantly evolving to stay ahead of the ever changing cyber threat landscape. Enabling secure customer access and protecting customer data are the primary goals of our information security program.

Over the past several years, the world has seen a huge increase in both the number and complexity of cyber attacks against governments and business enterprises. Regardless of the motivations behind these ever-changing threats, Neustar has taken the necessary steps to not only protect against these threats, but to stay ahead of them. Through a robust, defense-in-depth corporate information security strategy, which encompasses requisite preventive, detective, and corrective security measures, along with a proven Information Risk and Compliance program, Neustar is well prepared for these current and emerging cyber threats. These programs were designed to protect Neustar and our customer's information systems and data, while providing a secure means for customer access. Leveraging people, processes, and technologies, Neustar continuously assesses current capabilities against emerging threats and regularly updates security and privacy controls to ensure operational resiliency.

Neustar uses resources across the organization to quickly and effectively respond to information security threats. The following are highlights of some of our overarching principles and practices:



- **Defense-in-depth approach**—Neustar embraces a defense in in-depth or layered approach to security including strong physical, technical and administrative security controls. As shown in Exhibit 1.4-1, Neustar uses a diverse selection of security tools and vendors, which eliminates risk of any one vendor-specific security vulnerabilities.
- **Threat intelligence capability**—Neustar understands the ever-changing threat landscape and the increasing number of complex attacks being launched by hackers. In order to stay ahead of new attack methods, Neustar has implemented a "threat-intelligence" capability that provides us with improved zero-day (a previously unknown vulnerability in a computer application, meaning that the attack occurs on "day zero" of awareness of the vulnerability.) malware detection through advanced threat-feeds.
- **Security-Related Information**
- **Security-Related Information** Security-Related Information
- **Continued training and education**—Neustar's information security team keeps up with the latest security best practices, by attending training, conferences, and networking with other security professional in various companies via industry working groups, organizations, and events. In addition, our security experts provide mandatory annual Information Security Awareness training for the entire work force.
- **Industry best practices**—Neustar's information security and risk management program aligns with the ISO27001 standards and National Institute of Standards and Technology (NIST). Neustar is currently preparing for the ISO27001 certification for the NPAC. The NPAC infrastructure is currently ISO9001:2000 certified.
- **Security-Related Information**
- **Regular audits**—Neustar is subjected to regular audits such as: Sarbanes Oxley, SSAE16, ISO9001:2000, and self-imposed internal audits.

Security-Related Information

Security-Related Information

Security-Related Information

1.4.2 Information Security Framework

Neustar's Information Security Framework consists of sophisticated measures that both proactively defend against attacks as well as rapidly respond to them for minimizing the impact of any attack. **Security-Related Information**

Our detective and corrective measures are implemented and managed through the Neustar Cyber Incident Response Team/Security Operations Center (NeuCIRT/SOC).

Neustar's information security starts with comprehensive policies and standards utilizing industry best practices, including ISO and NIST. Policies and standards are reviewed semi-annually and updated as needed. Through adoption of recognized standards and the utilization of proven security solutions, Neustar has a cohesive and highly effective approach in protecting against data loss, targeted advanced persistent threats, and distributed denial of service attacks.

We have implemented enhanced security monitoring and threat prevention by developing a variety of techniques and systems to maintain awareness of emerging techniques and tools in the hacking community. **Security-Related Information**

Neustar recognizes the vital need to secure the systems and the integrity of the data in commercial solutions. Our extensive background in carrier-grade solutions has led us to install and operate computing and communications systems in accordance with solid business and security practices, including the consideration of physical, network, server, and application elements.

1.4.2.1 Information Security Framework—Preventive Controls

As the old saying goes, "an ounce of prevention is worth a pound of detection," preventive measures are always better than a cure. Preventive-based security controls provide a higher level of efficiency whereas detective and corrective based security control is usually much more costly. While Neustar maintains solid detective/corrective controls, the foundation of the security program (shown in Exhibit 1.4-2) is built on time-proven preventive controls (administrative and technical).

Security-Related Information

Security-Related Information

Endpoint Security

Neustar's security teams have deployed a comprehensive approach to security for the endpoint: employee desktops, laptops, and other devices. Employee desktops and laptops are one of the largest targets for hackers, viruses, and malware. To safeguard our endpoints, we have deployed proven technologies in a defense-in-depth approach, which directly increases the security posture of NPAC. Some of the key security capabilities that protect the NPAC environment include:

- Security-Related Information

Security-Related Info:

- Security-Related Information

Security-Related Info:

- **Security awareness training for the workforce**—Neustar firmly believes that employees are the first line of defense against security incidents; therefore, we have successfully developed a "culture of security" environment. Through specialized security and awareness training and focused security forums, employees are made aware of security-related threats and potential attack vectors (i.e. vulnerable applications, phishing attacks, social engineering, etc), thus providing an additional line of defense against malicious security activities.

- **Security-Related Information** eustar has deployed protections to block potential harmful and non

- Security-Related Information

- Security-Related Information

- **Network access control**—Neustar utilizes network access control (NAC). NAC gives us full visibility to every system on the network and allows us to limit access for different classes of users with the use of policies.

- Security-Related Information

Security-Related

- Security-Related Information

Operating Systems Security

To protect our operating systems, we utilize the following preventive system controls:

- Security-Related Information
- Security-Related Information
- **Patch management**—Neustar's formal patch management program was implemented to not only ensure timely security patching of systems, but also to provide improved system performance and compliance with regulatory requirements.

Identity Management Security

Neustar has implemented a comprehensive set of technologies to form our Identity and Access Management Program. This program has allowed us to centrally control the lifecycle of all identities in the NPAC. Security-Related Information

- Security-Related Information
- **Web access**—Neustar offers Web Access Management and Policy controls to ensure only authorized users can access protected resources and generate SSO tokens for seamless session experience. Security-Related Information
- **SSO**—Neustar offers a secure SSO capability to its partners or customers. Internal identity federation provides a standards-based approach to bridging identity silos and application domains. We support all federation standards such as SAML, OAuth, WS-Federation, STS, OpenID. **Security-Related Information**

Both scenarios offer users seamless resource access.

- **Centralized identity management—Security-Related Information**
This allows us to manage the life cycle of accounts more efficiently and gives us greater control over individual's access. Neustar practices the principle of least privilege for all accounts.
- **Two-factor authentication—Security-Related Information**

Security-Related Information



1.4.2.2 Information Security Framework—Detective and Corrective Controls

Cyber attacks by hostile organizations such as nation-states and organized crime are on the rise, which is threatening governments and corporations by attempting to steal strategic, technical, financial, and national security information. The increasingly sophisticated and aggressive nature of these attacks require equally assertive measures be taken to detect, respond, correct, and adapt quickly to these ever-changing cyber threats in order to protect critical information assets.

Security-Related Information



Security-Related Information

- Proactive threat research on emerging threats
- Security-Related Information
- Security-Related Information
- Focused reporting and briefings for advanced cyber threats and activity
- Security-Related Information

- Development of threat trend analysis reports and metrics
- Active participation in the security community including: meetings; training; seminar; conferences; associations, etc.
- Threat assessment reports of threat risks to programs, technologies, or systems, based on open and intelligence sources

The Neustar Difference

Neustar's role as a provider of mission-critical functions to entire industries; such as the LNPA, domain name registries, and UltraViolet digital rights and identity manager makes us an attractive target to attackers. Therefore, **Security-Related Information**



We've created identity management solutions that enable our users to access our services in a user-friendly manner while maintaining strict security control. We have created an environment that encourages constant training and rapid response through our regular security penetration testing.

1.4.3 Information Risk and Compliance

Neustar recognizes that effective security management includes not only technical and tactical defense, but also a security approach that encompasses security risk management and compliance to further strengthen Neustar's infrastructure.

With increasing global threats to financial and information related industries, Neustar has enhanced its current security program to include an IT Risk and Compliance group (ITRC)—see Exhibit 1.4-4. This is a group of highly skilled professionals with decades of information risk and compliance experience in the telecommunication, new media, Internet, and government sectors. **Security-Related Information**

In addition, the Business Continuity Management (BCM) program strategy (see Proposal Section 1.2.4) and execution is managed with oversight from the ITRC.

Security-Related Information

Security-Related Information

- **NPAC Technical Neutrality Audit**—Focus is on industry neutrality. Neustar provides a spotless record on neutrality and has passed all third-party audits of Neustar's neutrality. We are the only entity to have our neutrality confirmed in a Commission order.
- **NPAC Article 14 Audit**—Focus is on NPAC data center and operations in comparison with industry best practices. An independent, intensive third-party review of Neustar's NPAC data center and operations has found that these areas have consistently exceeded or far exceeded industry best practices in all tested areas year-over-year, including both Business Continuity Management and Security. See Exhibit 1.4-5 for our industry best performance record with regard to security for the NPAC.
- **ISO9001**—Focus is on NPAC's Quality Management System and documentation subject to a yearly external audit. Results from the annual ISO 9001 quality audits show consistent high performance and continual improvement.
- **Sarbanes-Oxley (SOX)**—Focus is on revenue, financially significant lines of business and systems. Neustar consistently has maintained a stable and compliant control environment, utilizing the COSO and COBIT frameworks. Since Neustar's public offering, Neustar has not had a materially significant deficiency found during any Section 404 testing for Sarbanes-Oxley.

Security—Article 14 Audit Scores

Category	2009	2012	Trend
Security Overall Score	4.50	4.50	↔
Security Governance	4.30	4.37	▲
<i>Security Policy</i>	4.30	4.50	▲
<i>Security Awareness Training</i>	4.40	4.40	↔
<i>Security Compliance</i>	4.20	4.20	↔
Firewall	Security-Related Information		↔
Remote Access			↔
Network Security			↔
Host Systems & Database Security			↔
Data Center Security			↔

- 5 - Excellent performance, far exceeds industry best practices
- 4 - Above average performance, generally exceeds industry best practices
- 3 - Average performance, meets industry best practices
- 2 - Below average performance, fails to meet industry best practices
- 1 - Poor performance, falls far below industry best practices

142.npac2013

Exhibit 1.4-5: Third-party audits validate our performance and provide valuable input on possible future enhancements.

- **Managing the Quality Management System (QMS)**—This is comprised of highly skilled information security risk and compliance specialists. The QMS ensures an objective, independent review of internal processes, controls, and practices across the enterprise. Our ISO 9001 certification validates the effectiveness of the QMS.
- **Leveraging third-party automated tools to ensure high-quality performance**—Neustar has implemented an industry-leading IT Governance, Risk, and Compliance (ITGRC) **Security-Related Information**. The use of such automated tools provides for further business agility while providing risk, vulnerability, compliance, business continuity, and disaster recovery metadata management and tracking.

Oversight not only includes information security, but also business processes, documentation, physical and environment controls, and other areas of the company that may have a downstream effect on the information and operational environments. Through a layered approach, Neustar's technical, administrative, and physical controls are designed to ensure Neustar's assets are properly protected, operate effectively, and remain in compliance with legal and regulatory requirements.

Information Security Risk Management

Neustar recognizes that security risk management is a critical component of its operations at the corporate and business unit levels. To properly manage corporate assets and to serve customers as expected, Neustar has incorporated regularly scheduled security risk assessments of its business units. The probability of each risk is assessed and an overall inherent risk rating is derived. The process considers both external and internal risk factors on each business unit, and management's capability to focus on the impact of those factors on operations. The findings from the information security risk assessments are distributed to our senior leadership and incorporated into the Neustar Enterprise Risk Management (ERM) reports, as required.

Neustar has implemented an integrated approach to information security risk management throughout the enterprise. Under the leadership of **Security-Related Information**, the information security risk management teams are well positioned to provide the requisite oversight to ensure risk-benefit analyses, and security are applied throughout the risk management process. Neustar's assessment methodology is based on industry specifications such as ISO27001, ISO27005 (shown in Exhibit 1.4-6), and the newer ISO31000 standards, which allows for a comprehensive approach to be applied in the evaluation of mission security risks, including the identification of proper protections to safeguard information systems and customer data.

- **Security-Related Information**

Security-Related Information

- Security-Related Information

2.3 Neustar's Neutrality



Why Neustar

- Meets or exceeds all VQS and RFP Neutrality Criteria today
- Neutrality Code of Conduct, developed in collaboration with the FCC and Industry, is in place today
- Successful, corporate-wide Neutrality Compliance Program in place today
- More than 60 numbering-related neutrality audits passed since Neustar's creation in 1998
- Neutrality Legal Opinion provided by an independent law firm with more than a decade of experience in reviewing LNP neutrality
- Long history of neutrality can give Industry confidence of neutrality continuing into the future
- No complex or time-consuming neutrality cure required

VQS Section 3.4 requires that the Primary Vendor and all Subcontractors must "at all times be Neutral Third Parties" and the RFP requires each of the regional LNP databases be managed by an LNPA that is "neutral and independent from Telecommunications Carriers." Further, the RFP Section 4.2 requires an audit of an LNPA's neutrality to be conducted every six months.

Neustar has an unquestioned record of neutrality in numbering administration that simply cannot be matched by any other entity. Created in 1998 specifically to be assigned North American Numbering Plan Administrator and LNPA contracts from the non-neutral Lockheed Martin, Neustar was born into an environment that mandated neutrality from telecommunications numbering administrators. From the outset, Neustar made neutrality an integral part of its corporate essence. Neustar was a Neutral Third Party when it was created in 1998 and Neustar remains a Neutral Third Party today. Indeed, Neustar's very name is a constant affirmation of the company's continuing commitment to neutrality.

Neutrality, though, is more than just a name. Neutrality in numbering administration must be lived in practice constantly, not merely practiced when convenient. Since 1999, Neustar has been governed by a Neutrality Code of Conduct that was developed in consultation with the Commission and the Industry. This Code of Conduct was included in the Commission order approving the transfer of the NANPA contracts from Lockheed Martin to Neustar and was referenced in the agreement by which the Industry approved the assignment of the LNPA agreements to Neustar. To Neustar's knowledge, this is the only such Code of Conduct in existence today.

NEUSTAR CODE OF CONDUCT

1. Neustar will never, directly or indirectly, show any preference or provide any special consideration to any company that is a telecommunications service provider, which term as used herein shall have the meaning set forth in the Telecommunications Act of 1996.
2. No shareholder of Neustar shall have access to user data or proprietary information of the telecommunications service providers served by Neustar (other than access of employee-shareholders of Neustar that is incident to the performance of NANPA and LNPA duties).
3. Shareholders of Neustar will ensure that no user data or proprietary information from any telecommunications service provider is disclosed to Neustar (other than the sharing of data incident to the performance of NANPA and LNPA duties).
4. Confidential information about Neustar's business services and operations will not be shared with employees of any telecommunications service provider. Neustar shareholders will guard their knowledge and information about Neustar's operations as they would their own proprietary information.
5. No person employed by, or serving in the management of any shareholder of Neustar will be directly involved in the day-to-day operations of Neustar. No employees of any company that is a telecommunications service provider will be simultaneously employed (full-time or part-time) by Neustar.
6. Warburg Pincus will not control more than 40% of Neustar's Board.
7. No member of Neustar's board will simultaneously serve on the board of a telecommunications services provider.
8. No employee of Neustar will hold any interest, financial or otherwise, in any company that would violate the neutrality requirements of the FCC or the NPAC Contractor Services Agreements (the Master Agreements).
9. Neustar will hire an independent party to conduct a neutrality review of Neustar, ensuring that Neustar and its shareholders comply with all the provisions of this Code of Conduct. The neutrality analyst will be mutually agreed upon by Neustar, the FCC, NANC and the LLCs. The neutrality review will be conducted quarterly. Neustar will pay the expenses of conducting the review. Neustar will provide the analyst with reasonable access to information and records necessary to complete the review. The results of the review will be provided to the LLCs, to the North American Numbering Council and to the FCC and shall be deemed to be confidential and proprietary information of Neustar and its shareholders.

To ensure Neustar's compliance with the Neutrality Code of Conduct, the Code requires Neustar to undergo quarterly neutrality audits by a mutually agreed third party. Thus, Ernst & Young has conducted 50 quarterly reviews of Neustar's compliance with the Code of Conduct and other neutrality rules. Each of those 50 quarterly audits confirmed Neustar's continuing neutrality and these audit reports are shared with the Commission, the NANC, and the NAPM LLC. Moreover, beginning in 2003, the law firm of Piper Rudnick, now known as DLA Piper, conducts annual neutrality audits and submits its findings to the NAPM LLC. Each of these 10 annual audits has also confirmed Neustar's compliance with the Code of Conduct. No other prospective vendor has ever been subjected to such rigorous neutrality audits.

Below, Neustar will discuss the continuing importance of neutrality in the LNPA and then explain its neutrality compliance program in greater detail.

Neutrality Remains Critical to the Success of Local Number Portability

Neutrality in telecommunications numbering administration is not an idle academic exercise. The requirement in the Telecommunications Act of 1996 that the Commission "create or designate one or more impartial entities to administer telecommunications numbering" originated out of concern that telephone numbers were such an integral component of a telecommunications service that a biased administrator could impede the development of telecommunications competition. With this directive from Congress, and sharing the Congressional concern, the Commission, in FCC 96-286 at ¶192, determined that it was in the "public interest for the number portability databases to be administered by one or more neutral third parties." The Commission continued:

Neutral third party administration of the databases containing carrier routing information will facilitate entry into the communications marketplace by making numbering resources available to new service providers on an efficient basis. It will also facilitate the ability of local service providers to transfer new customers by ensuring open and efficient access for purposes of updating customer records. . . . Neutral third party administration of the carrier routing information also ensures the equal treatment of all carriers and avoids any appearance of impropriety or anti-competitive conduct. Such administration facilitates consumers' access to the public switched network by preventing any one carrier from interfering with interconnection to the database(s) or the processing of routing and customer information. Neutral third party administration would thus ensure consistency of the data and interoperability of number portability facilities, thereby minimizing any anti-competitive impacts.

When those words were written in 1996, competition in the local telecommunications market was still a vision. Fax machines and pagers were prominent. There were clear distinctions between Service Providers who were RBOCs, CLECs, IXC's, CMRS providers, and cable operators. There were only 60 million wireless subscribers in the United States and wireless Service Providers were initially exempt from the Telecommunication Act's LNP requirements. There were no smart phones. SMS and MMS were not in widespread use. The ITU-T had only just begun the development of standards for the transmission and signaling of voice communications over Internet Protocol (VoIP) networks with the H.323 standard.

Today, in part because of LNP, the telecommunications marketplace in the U.S. has grown into the largest and most competitively robust market in the world as traditional companies, cable operators, mobile providers, and new entrants square off to compete for business and residential subscribers. Wireless is exploding: there are now 330 million wireless subscribers in the U.S. and more SMS and MMS messages are sent each month than voice calls are made. New mobile devices are appearing in the market with increasing velocity; seemingly, everyone today has a smart phone, a tablet, or both. There are hundreds of thousands of applications available for these devices and millions are downloaded each day. VoIP is commercially available and in use by consumers and corporations throughout the country.

Innovation and change are the norm for the U.S. telecommunications market now and will be in the future. New handset devices are still being launched. More tablets and other devices are being developed. Convergence in voice, text, video, and Internet is increasing. Service providers are in the middle of developing and executing LTE plans and implementations. With this innovation and change, local number portability is more important today than ever. There are more than 600 million TNs contained across the seven regional NPAC/SMS systems. More than 500 million NPAC/SMS transactions occurred in 2012 alone. The NPAC/SMS enables number conservation using Thousands-Block Pooling and is readily used by Service Providers to gain customers, retain customers, migrate customers to different networks, and to restore service to customers in the event of outages or disasters. Neustar, as the U.S. LNPA, processed billions of individual Common Management Information Protocol (CMIP) operations in 2012 in support of those 500 million NPAC/SMS transactions.

With the continuing importance of local number portability, even a relatively small failure in the administration of LNP would have a significant financial impact on carriers and damage consumer confidence in a system that is a linchpin for telecommunications competition. As the Industry knows, the NPAC/SMS is an extremely complex system the performance of which is instrumental in ensuring the success of LNP in enabling the delivery of every voice call and text message, and the provision of critical services such as telephone number management and the restoration of service in the event of a disaster. The NPAC/SMS is a critical part of the telecommunications infrastructure in the United States. Confidence in the neutrality of the LNPA is critical, not only because the LNPA is privy to competitively sensitive information, but also because all participants in the Industry must be able to trust the LNPA to operate in a manner that will not favor any particular Service Provider or Industry segment, particularly as the LNPA and Industry adapt the NPAC/SMS to accommodate the Industry's transition to all-IP networks,

A Neutral Third Party administrator is essential to ensuring consumers and businesses are able to switch Service Providers without obstruction or undue delay in the process. Positive experiences with the porting process by consumers and businesses are vital to the success of communications competition. If consumers and businesses encounter unreasonable delays in their attempts to change Service Providers or if changing providers becomes an intolerable hassle, consumers and businesses will then become less likely to attempt switching providers. Thus, communications will be compromised if an LNPA, because of corporate affiliations or contractual relationships, acts in a non-neutral fashion. A non-neutral administrator may choose not to adequately support complex mass migration transactions or may selectively enforce transaction processing rules and Industry guidelines to give favored carriers or favored segments a competitive advantage. Similarly, since the LNPA and NPAC/SMS can play a major role in disaster recovery, a favored Service Provider could offer assurances to consumers and businesses that their services will be restored more rapidly than others after a natural disaster.

The LNP administrator must also be able to represent the porting interests of the Industry at standards development committees impartially. A biased administrator can use its power to block or push for standards for the benefit of one customer or Industry segment. Indeed, such an administrator could change feature functionality of the NPAC system to benefit certain providers or Industry segments, such as by supporting certain technologies over others. This is the very essence behind the requirements that a numbering administrator not be aligned with any particular Industry segment.

The Industry must be able to trust the integrity and neutrality of its LNPA for local number portability to function as intended. The porting process necessarily requires that Service Providers share confidential customer information and proprietary business plans with the LNPA. Service providers must have confidence that their competitively sensitive information will be tightly guarded and not shared with one or more of their competitors. If Service Providers lose this confidence because of real or perceived neutrality concerns with the LNPA, the entirety of the local number portability system will cease to function efficiently. If the portability system breaks down, then non-favored Service Providers may lose business because they can no longer capture new customers, leading not only to diminished communications competition but also to reduced consumer benefit that flows from vibrant competition. Moreover, the mere perception that the LNPA is favoring an Industry member or segment, or has the incentive to do so, will result in the Commission, the NAPM, and carriers devoting increased resources to monitoring the LNPA.

Given the increasing size of the U.S. communications market, the increasing level of competition, the increasing reliance on LNP for use beyond just competitive porting, and the volume of work the U.S. LNPA has to perform, the neutrality of the U.S. LNPA is more important than ever before and will be even more important in the future.

Neustar's Unmatched Commitment to Neutrality

Commitment to neutrality in numbering administration permeates all aspects of Neustar's corporate existence. Neustar's Restated Articles of Incorporation, its corporate bylaws, and even its stock certificates all contain provisions reflecting the neutrality requirements imposed on Neustar by the Commission and the Industry. Neustar views every relationship that it undertakes, acquisition that it contemplates, investment that it examines, and debt that it incurs through the prism of neutrality. Contracts are declined; acquisitions and investments refused; and neutrality provisions negotiated into Neustar's debt instruments. No other company can make these claims, just as no other company can fully appreciate the full scope of what number administration neutrality entails.

Several examples are illustrative. In the winter of 2010, Neustar entered into merger discussions with Syniverse, Inc. During the course of due diligence between the two companies, Neustar discovered that Syniverse held Certificates of Public Necessity and Convenience (or equivalent authority) to provide telecommunications services in 32 states. In addition, Syniverse had tariffs on file in several states for the provision of SS7 and private line services, and had filed and paid state taxes based on telecommunications revenues in several jurisdictions. Finally, Neustar found that Syniverse held a license issued under section 214 of the Commission's rules that indicated Syniverse was a common carrier.

Because of its neutrality obligations as the LNPA, the NANPA, and the PA, Neustar refused to enter into a definitive merger agreement with Syniverse until Syniverse was no longer providing any telecommunications services and had removed all indicia of being a Telecommunications Service Provider (TSP). Syniverse requested a definitive agreement *before* resolving its TSP issues, a condition that Neustar found incompatible with our neutrality obligations as the LNPA, NANPA, and PA. Discussions on the potentially lucrative merger broke down.

Six months later, Syniverse placed itself up for sale through an auction process. The starting point for the bidding was several billion dollars above the price that had been discussed only months earlier with Neustar. Neustar participated in the bidding because we believed that there would still be value for our shareholders and because it appeared that Syniverse had addressed the neutrality concerns arising in the previous negotiation. However, the acquisition was again impacted by the neutrality rules that apply uniquely to Neustar. Based on the then in effect interpretation of the FCC's neutrality rules, Neustar was required to obtain Commission approval prior to obtaining debt from any TSP affiliate—a requirement that would cover virtually every lender of any size. The public nature of this approval process imposed a burden of transparency on Neustar's financing capacity to which other bidders for Syniverse were not subjected, affecting the auction process. Syniverse ultimately sold itself to the Carlyle Group. A case could be made that neutrality deprived Neustar's investors of the benefits of the Syniverse merger, but Neustar understands that this is just part of its responsibility as a Neutral Third Party numbering administrator.

The Syniverse example, while large, is not an isolated occurrence. Neustar periodically looks to make investments in new companies that are developing promising new technologies, in part to help Neustar develop interesting new products that it can deliver to the communications industry. Each of these potential investments is investigated to ensure the target company is not a TSP or a TSP affiliate. Moreover, even if the company satisfies that check, Neustar requires that a neutrality escape clause be negotiated in its investment agreement, so that Neustar will be bought out immediately if the target company becomes a TSP or TSP affiliate in the future. Unfortunately, a number of the companies in which Neustar has sought to make such investments have not wanted to be encumbered by the neutrality driven provision and the investments could not be made.

The neutrality rules also affect entities that invest in Neustar. Pursuant to the Commission neutrality rules that apply to the NANPA and the PA, no TSP or TSP affiliate is permitted to own more than 5% of Neustar's equity. Rather than waiting for its investors to file documentation with the Securities and Exchange Commission (SEC) indicating that their ownership went above the 5% threshold, filings that can lag significantly in time, Neustar actively monitors its investors' ownership stakes using third-party services. As soon as Neustar discovers an investor has reached a 5% ownership stake, Neustar contacts the investor to ask for certification that it is not a TSP or a TSP affiliate, that is, that the investor itself is not on the Commission's list of TSPs (Form 499 list) nor does it own 10% or more of any entity that appears on that list. If they are not able or willing to provide such a certification, Neustar asks that the investor either reduce its investment in any TSP to below a level below 10% and provide the certification, or maintain its TSP investment but reduce its investment in Neustar to below 5%. Most investors that cross the 5% Neustar investment threshold have been able to provide Neustar with certification that they are neither TSPs nor TSP affiliates. In other instances, however, investors have chosen to draw down their TSP investments and, in others, reduce their stake in Neustar.

From a major transaction such as the Syniverse proposed merger, to the occasional investment opportunities that must be reviewed, to the standard day-to-day monitoring of our investors, Neustar's commitment to neutrality is clear and unmatched.

Neustar is the only vendor in the industry with an effective and comprehensive neutrality compliance program in place today to ensure our Neutrality through the next contract term.

Neustar has been able to undergo the extensive scrutiny of its neutrality auditors without significant issue because it has a comprehensive neutrality compliance program in place throughout the company. Overseeing Neustar's neutrality is the Neutrality Committee of Neustar's Board of Directors. This committee, composed of Neustar's CEO and two independent board members, establishes the company's neutrality compliance program and reviews the

reports of the neutrality auditors. The committee adopted the Neustar Neutrality Compliance Procedures, which provides a plan for compliance with the Neustar Code of Conduct, the Commission's neutrality orders and regulations governing the NANPA, PA and LNPA, and the current LNPA Master Agreements. Reporting to this committee and responsible for implementing the Neutrality Compliance Procedures and handling day-to-day neutrality issues is Neustar's Neutrality Officer, currently John Manning.

Neustar's neutrality compliance procedures begin with neutrality training for every one of Neustar's employees and directors, no matter where located or how removed from numbering administration. Employees and directors first undergo neutrality training as part of their onboarding process into the company and then go through a mandatory neutrality training program once a year thereafter. Additionally, prospective directors are vetted for neutrality before being permitted to join Neustar's Board of Directors. Employees and directors are required to certify their neutrality when they begin employment and their continuing neutrality every quarter thereafter.

Neustar feels that it is critical all employees and directors are given this training and required to provide the certifications because neutrality issues can arise in a number of ways, and given the global nature of communications, can come up anywhere in the world. All employees must understand Neustar's neutrality obligations so that we can avoid violations and so the employees can bring potential neutrality issues to the attention of the Neutrality Officer. For example:

A Neustar employee in Europe who may want to make an investment in a European company needs to understand that Neustar must be assured that the target company is not and will not become an affiliate of a U.S. TSP. Similarly, in 2011, a Neustar finance department employee recognized a potential neutrality issue when she received a notice of a Service Provider's annual meeting. Because of her neutrality training, she immediately brought the issue to the attention of the Neutrality Officer. It was determined that Neustar had inadvertently become the holder of a small number of shares of this SP, possibly as the result of a bankruptcy settlement in favor of a company acquired by Neustar. Because the Neustar employee recognized the neutrality issue, Neustar was able to notify the Commission and its auditors of the issue, and quickly disposed of the Service Provider's shares by donating them to the American Red Cross. Corporate-wide neutrality compliance training enables the prevention of neutrality issues before they occur and the rapid identification and resolution of such issues if one does occur.

The quarterly neutrality certifications by Neustar's employees and directors, along with a quarterly neutrality certification submitted by Neustar's CEO on behalf of the company, are an important part of the neutrality audits that Neustar undergoes. These audits, which cover all of Neustar, are performed annually in accordance with Neustar's current NPAC contract and quarterly as part of Neustar's NANPA and PA contracts. As noted above, the audits review Neustar's compliance with the Neutrality Code of Conduct, developed in collaboration with the Commission and the Industry, and with the Commission's rules and orders and the LNPA Master Agreements. In the course of the audits, Neustar makes available the necessary documents for the auditors including: neutrality compliance certifications from each employee, board member, and executive officer; a management assertion letter and management compliance certification; new hire certifications; and the results of the neutrality tests given annually to every Neustar employee. The auditors also review LEAP service agreements, NPAC end user agreements, NPAC access and security, and customer transactional documentation from the NPAC, NANPA, and PA to ensure Neustar has treated each user or applicant fairly and in an unbiased manner. The auditors review certifications from each



shareholder holding a 5 percent or greater share of Neustar's outstanding stock, notices to the FCC of any organizational and board changes, as well as our debt and revenue information. Our auditors then conduct extensive internal review of the audit proceedings, findings, and reports to ensure all appropriate audit procedures were followed.

The auditors' reports are reviewed by the Neutrality Committee of Neustar's Board of Directors. The full Board of Directors also reviews the results of the audits for independence, integrity, accuracy, and irregularities, and certifies its acceptance of the audit report by attesting and forwarding it to the FCC's Wireline Competition Bureau, Enforcement Bureau, the NANC, and the NAPM LLC.

As noted above, the results of this corporate-wide focus on neutrality speak for themselves. To date, Neustar has passed all 10 annual LNPA Neutrality Audits and all 50 quarterly NANPA/PA Neutrality Audits. In the highly competitive and volatile communications Industry, this is a significant achievement. Congress anticipated the neutrality challenges facing numbering administrators when it mandated that such administrators must be impartial. Neustar faces those challenges every day. Neustar's seasoned and highly expert team minimizes those challenges and, when they arise, effectively addresses all such neutrality challenges to the satisfaction of the FCC and the Industry. Neustar will continue to place the highest importance on our neutrality compliance during the new contract term so that the NAPM and the FCC can be confident that the Industry can trust its LNP administrator not to allow its business relationship or close ties with Industry members or an Industry segment to override its obligation or cloud its judgment.

The Neutrality Legal Opinion provided by DLA Piper confirms Neustar's compliance with the Neutrality Criteria set forth by the NAPM LLC without requiring Neustar to make any structural or procedural changes. No complex neutrality cure that may require a time-consuming approval process is needed for Neustar to continue to serve as the U.S. LNPA.

DLA Piper LLP has furnished a Legal Opinion confirming Neustar's compliance with the Neutrality Criteria set forth in the Section 3.4 of the VQS. By mutual agreement between Neustar and the NAPM LLC, DLA Piper has for the last 10 years evaluated Neustar's compliance with neutrality requirements and so is uniquely qualified to issue a Legal Opinion regarding Neustar's neutrality. Better than any other law firm could, DLA Piper understands what to evaluate, the questions to ask, and the issues to raise in connection with an entity's compliance with the unique requirements for LNP neutrality. It is also important to note that these periodic neutrality audits represent the only business relationship that DLA Piper has with Neustar. Thus, DLA Piper truly is a neutral third party auditor, as it can evaluate Neustar's neutrality without any fear of losing other business.

The DLA Piper Legal Opinion does not require Neustar to make any structural changes to its corporate structure or make any other changes in order to be a Neutral Third Party. Because Neustar meets or exceeds the Neutrality Criteria, and because Neustar is not proposing the use of any subcontractors to provide LNPA services for the next contract term, neither Neustar nor any Neustar subcontractor must develop and adhere to any complex neutrality cure. Thus, when considering Neustar for the next LNPA contract term, the NAPM and the Commission will not have to evaluate the efficacy of a neutrality cure, a time and resource intensive effort. When Lockheed Martin announced its intent to purchase a subsidiary of COMSAT 1998, for example, it took approximately eleven months for the Commission and the Industry to resolve the neutrality issues satisfactorily.